REMARKS

Claims 1-12 are currently pending, wherein claim 10 has been amended to correct a typographical error in the previous amendment. Favorable reconsideration is respectfully requested in view of the remarks presented herein below.

In paragraph 3, the Office Action objects to claim 10 because the phrase "it blocks" in line 2 should be deleted. Claim 10 has been amended to correct the typographical error in the previous amendment, thereby addressing the Examiner's concerns.

In paragraph 5, the Office Action rejects claims 1-8 and 10-12 under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 6,094,724 to Benhammou et al. ("Benhammou"). Applicant respectfully traverses this rejection.

It is well known that in order to support a rejection under 35 U.S.C. §103, the applied reference(s) must teach each and every claimed limitation. In the present case, claims 1-8 and 10-12 are not rendered unpatentable over Benhammou for at least the reason that Benhammou fails to disclose or suggest a control counter as claimed.

Independent claim 1 defines a method of controlling the use of a smart card which includes a microprocessor and at least one control counter. The method includes, *inter alia*, the steps of decrementing or incrementing the control counter by one unit at the start of a transaction comprising at least one authentication session by the card, and if the authentication by the card is successful, subsequently incrementing or decrementing, respectively, the control counter by one unit.

Benhammou discloses a secured memory which provides an authentication protocol for anti-wire tapping and different password sets for reading and writing to secured memory areas by a secured memory user. The system of Benhammou includes an authentication zone partitioned into an Authentication Attempts Counter (AAC), an Identification Number, and a Cryptogram. The AAC is an eight bit counter that prevents a systematic attack on the authentication protocol that may be required before access to selected User Zones is permitted. According to Benhammou, each time the authentication protocol is run, the AAC is incremented. Furthermore, each time the authentication protocol is successful, the AAC is reset to zero (see Column 4, lines 54-65 of Benhammou). However, Benhammou fails to disclose or suggest that the AAC is decremented by *a unit* if the authentication protocol is successful as claimed.

In the rejecting claim 1, the Office Action asserts that Benhammou discloses decrementing the control counter as claimed inasmuch as Benhammou discloses resetting the AAC to zero each time the authentication protocol is successful. More specifically, the Examiner asserts that resetting the counter to zero is equivalent to decrementing the counter to zero. This assertion is unfounded for the following reason.

First, disclosing that a counter is reset to zero is not equivalent to disclosing that the counter is decremented. Resetting a counter to zero is an action with can be achieved by one or multiple steps, for example, each bit in the memory storing the counter value could be re-written with a zero in a single write function or in multiple write functions. Therefore, resetting the counter of Benhammou does not necessarily including decrementing the counter to zero as asserted by the Examiner. Furthermore, resetting a

counter implies that no matter what the value of the counter it is replaced with zero, in contrast to decrementing a counter which implies decreasing the value by a specified amount (in this case one unit) leaving a value which is not necessarily zero. Therefore, while decrementing the counter may achieve the result of resetting the counter to zero, resetting the counter to zero does not necessarily flow from decrementing the counter.

Second, independent claim 1 recites the counter is incremented/decremented by *one unit* each time an authentication session is started and decrementing/incrementing the counter by *said unit* if the authentication is successful. Accordingly, the counter of the invention is decremented by *one unit* whereas the counter of Benhammou is reset to zero, losing all track of previous failed sessions.

As discussed in the specification, a new type of fraud, referred to as differential power analysis (DPA), has appeared which consists of deducing the value of the secret keys in a smart card from statistical analysis based on measuring current consumption in the card during cryptographic calculations periods. This differential power analysis is carried out by initiating a cryptographic calculation with the same key numerous times, for example 300 times, and then aborting the transaction by removing the card. If the counter of the present invention was *reset* each time an authentication session was successful, there would be no record of the number of attempts made previously. Accordingly, differential power analysis could potentially be carried by a fraudulent user. In contrast, the present invention only decrements the counter by one unit such that any fraudulent attempts to manipulate the card remain.

Claims 2-8 and 10-11 variously depend from independent claim 1. In addition, independent claim 12 defines a smart card that includes, *inter alia*, a microprocessor that executes the method of claim 1. Therefore, claims 2-8 and 10-12 are patentably distinguishable over Benhammou for at least those reasons presented above with respect to claim 1.

In paragraph 6, the Office Action rejects claim 9 under 35 U.S.C. §103(a) as allegedly being unpatentable over Benhammou in view of Applicant's Admitted Art ("Admitted Prior Art"). Applicants respectfully traverse this rejection.

Claim 9 depends from independent claim 1. Therefore, claim 9 is patentably distinguishable over Benhammou for at least those reasons presented above with respect to claim 1. The Admitted Prior Art fails to disclose or suggest a control counter as claimed. To the contrary, as clearly stated on page 3, line 22, the session counter of the Admitted Prior Art is *irreversibly* incremented during the transaction. Accordingly, the Admitted Prior Art fails to overcome the deficiencies of Benhammou.

Since Benhammou and the Admitted Prior Art both fail to disclose or suggest a control counter as claimed, the combination of these two references cannot possibly disclose or suggest said element. Therefore, even if one skilled in the art were motivated to combine Benhammou and the Admitted Prior Art, the combination would still fail to render claim 9 unpatentable. Accordingly, Applicants respectfully request reconsideration and withdrawal of the rejection of claim 9 under 35 U.S.C. §103.

This application is in condition for allowance. Notice of same is earnestly solicited. Should the Examiner have any questions regarding this application, she is invited to call the undersigned at the telephone number provided below.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: December 16, 2003

By: Penny L Caudle
Penny L. Caudle
Registration No. 46,607

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620